MENGGUNAKAN INFORMATION RIGHTS MANAGEMENT (IRM) SEBAGAI BAGIAN DARI PENGENDALIAN PREVENTIF PADA SISTEM INFORMASI AKUNTANSI ORGANISASI PUBLIK

Siswanto
siswanto@pknstan.ac.id
Politeknik Keuangan Negara STAN

Raditya Hendra Pratama
h3ndra@pknstan.ac.id
Politeknik Keuangan Negara STAN

ABSTRAK

Penelitian ini bertujuan untuk mengetahui apakah IRM dapat digunakan untuk mengamankan informasi yang dibuat menggunakan aplikasi MS. Office dan dikirim melalui email serta menganalisis siklus pendapatan serta mengidentifikasikan pengendalian internal atas siklus pendapatan yang telah diterapkan di perusahaan. Metode yang digunakan dalam penelitian ini adalah melakukan studi literatur dengan cara mengumpulkan data melalui buku. Hasil penelitian menunjukkan bahwa IRM merupakan salah satu solusi cepat yang dapat diimplementasikan untuk mengatasi masalah penyalahgunaan informasi. Hal ini berlaku dalam skala kecil seperti individu maupun dalam skala yang besar seperti sebuah organisasi. Pemanfaatan IRM organisasi publik dapat memberikan perlindungan tambahan yang memadai terhadap distribusi informasi-informasi penting yang bersifat rahasia.

Kata Kunci: Informasi, akuntansi, pengendalian, keamanan, publik

PENDAHULUAN

Kebocoran informasi yang bersifat sensitif/rahasia dapat sangat merugikan bagi suatu organisasi serta memberikan dampak yang luas pada aspek bisnis, kepegawaian, pelanggan, dan rekanan (Lieberman, 2009). Oleh karena itu suatu organisasi harus melindungi diri dari terjadinya kebocoran informasi baik yang memiliki unsur kesengajaan ataupun yang bersifat kelalaian dari penerima informasi.

Menurut Lieberman (2009) sebagai hasil atau konsekuensi dari bocornya informasi penting dapat berupa beberapa hal merugikan bagi organisasi seperti berikut:

i. Kerugian secara finansial.
ii. Depresiasi/rusaknya kredibilitas dan nama baik di mata pelanggan ataupun rekanan.
iii. Kehilangan kesempatan bersaing dengan kompetitor.

Tujuan penelitian ini adalah sebagai berikut:

1. Mengetahui bagaimana IRM dapat digunakan untuk mengamankan informasi yang dibuat menggunakan aplikasi MS. Office dan dikirim melalui email.
2. Menganalisis siklus pendapatan serta mengidentifikasikan pengendalian internal atas siklus pendapatan yang telah diterapkan di perusahaan.

KERANGKA TEORI

Sistem Informasi Akuntansi

Menurut Romney dan Steinbart (2014) sistem adalah serangkaian dua atau lebih komponen yang saling terkait dan berinteraksi satu sama lain. Suatu sistem diciptakan untuk mencapai tujuan.Sistem ini terdiri dari subsistem yang lebih kecil untuk mendukung sistem yang lebih besar. Semakin besar suatu organisasi, semakin kompleks pula sistem yang digunakan. Pengertian akuntansi menurut Romney dan Steinbart (2014) adalah data yang telat diolah dan diproses. Informasi berfungsi untuk memberikan arti dalam hal proses pengambilan keputusan. Sebuah organisasi membutuhkan informasi untuk membuat keputusan yang efektif. Akuntansi adalah suatu proses mengidentifikasi, mengumpulkan, mencatat, menyimpan dan mengolah data. Menurut Waren, Reeve dan Duchac (2011), akuntansi dapat didefinisikan sebagai suatu sistem informasi yang memberikan laporan kepada pengguna tentang kegiatan ekonomi dan usaha.Akuntansi juga dapat dikatakan sebagai bahasa atau instrumen bisnis yang sangat berguna bagi pengguna internal maupun eksternal.Akuntansi dapat memberikan informasi secara berkala bagi pengguna dalam mengambil keputusan.

Dari pengertian-pengertian di atas, dapat disimpulkan pengertian sistem informasi akuntansi.Terdapat beberapa ahli yang telah mengemukakan pendapatnya mengenai pengertian sistem informasi akuntansi. Romney dan Steinbart berpendapat bahwa sistem informasi akuntansi adalah suatu sistem yang terdiri dari kegiatan mengumpulkan, mencatat, menyimpan dan mengolah data untuk menghasilkan

informasi bagi pengambil keputusan. Unsur dari sistem ini meliputi orang, prosedur dan instruksi, data, perangkat lunak, instruktur teknologi informasi, serta pengendalian internal dan ukuran keamanan. Sementara itu, menurut Hall (2016), sistem informasi akuntansi adalah suatu sistem yang tersusun atas tiga subsistem besar, yaitu : (1) *transaction processing system (TPS)*, yang membantu mengoperasikan bisnis dengan berbagai laporan dan dokumen antar bagian organisasi, (2) *general ledger/financial reporting system (GL/FRS)*, yang menghasilkan laporana keuangan seperti laporan laba rugi, neraca, laporan arus kas, dan laporan lain yang dibutuhkan, dan (3) *management reporting system (MRS)*, yang menyediakan laporan manajemen internal dalam pengambilan keputusan.

Menurut Romney dan Steinbart (2014), sistem informasi akuntansi dapat diterapkan dalam siklus bisnis suatu perusahaan. Siklus ini terdiri dari siklus pendapatan, pengeluaran, produksi, menajemen sumber daya manusia dan penggajian, serta sistem buku besar dan pelaporan. Kelima sistem tersebut akan saling berhubungan satu dengan yang lainnya untuk mencapai tujuan perusahaan yang sudah ditetapkan. Masing-masing dari siklus bisnis tersebut memiliki prosedur dan sistem pengendalian yang berbeda-beda.

Deskripsi IRM

Menurut Pemerintah Queensland (2008) Information Rights Management (IRM) adalah komponen/feature yang disediakan untuk memberikan layanan berupa kemungkinan bagi penulis dokumen untuk mengatur siapa yang dapat membaca dokumen mereka dan apa yang dapat dilakukan terhadap dokumen tersebut serta kapan hal tersebut dapat dilakukan.

Tanpa IRM, dokumen elektronik yang beredar tidak dapat dikontrol dan dapat dicetak, disalin, dan diteruskan secara bebas kepada siapa pun. Pengiriman informasi melalui email dan melewati jaringan yang aman dapat melindungi informasi pada area transit (tujuan) dokumen tersebut, tetapi tidak memberikan kontrol atas apa yang dilakukan oleh penerima dokumen terhadap informasi tersebut.

Menurut Pemerintah Queensland (2008) IRM dapat digunakan untuk mencegah pencetakan atau penyampaian informasi dalam email dan untuk

membuat informasi tersebut tidak dapat diakses oleh penerima setelah tanggal kedaluwarsa yang telah ditetapkan. IRM mampu membuat oleh orang lain selain dari penerima yang ditentukan tidak dapat membaca dokumen yang berisi informasi tersebut.

Peran Penting IRM

Menurut Lieberman (2009) IRM dapat membantu suatu organisasi untuk memenuhi dua kebutuhan fundamental berikut:

i. Membatasi akses untuk informasi yang bersifat sensitif/terbatas/rahasia.

ii. Memberikan kontrol terhadap informasi yang bersifat rahasia sekaligus memberikan nilai terhadap integritas informasi tersebut.

Menurut Yang Yu dari Stony Brook University, organisasi yang ada pada saat ini mulai serius dalam menerapkan keamanan informasi dalam jaringan organisasi mereka. Kebanyakan organisasi sudah mulai menggunakan sistem keamanan seperti *firewall, log-in security*, dan teknologi lainnya untuk melindungi properti/aset intelektual organisasi. Namun demikian, perlu disadari bahwa teknologi keamanan jaringan tersebut memberikan batas keamanan dari pihak luar yang tidak dikehendaki untuk melakukan akses kepada informasi dalam jaringan organisasi tetapi tidak membatasi aktor-aktor dalam organisasi untuk melakukan apa saja terhadap informasi yang mereka peroleh termasuk membocorkan informasi tersebut kepada pihak-pihak yang tidak berwenang atau bahkan dilarang memperoleh informasi tersebut (Infosys Limited, 2010).

Dengan keadaan tersebut di atas, maka kemudian disadari bahwa keamanan tidak hanya perlu dibangun dalam jaringan organisasi tetapi juga dalam informasi yang menjadi aset organisasi agar tetap menjadi *in-house information* dan tidak menyebar ke pihak-pihak yang tidak berwenang dan tidak berkepentingan.

Menurut Yang Yu dari Stony Brook University IRM dinilai dapat memberikan solusi cepat untuk menjaga informasi rahasia dari akses dan penyalahgunaan pihak-pihak yang tidak berwenang baik dari dalam maupun luar organisasi. IRM dapat meminimalisasi potensi penyalahgunaan informasi melalui mekanisme *forwarding, copying,* dan pencetakan informasi tersebut dalam bentuk fisik. Hal tersebut

dilakukan dengan menonaktifkan fungsi-fungsi tersebut sehingga tidak dapat dilakukan kecuali dengan izin dari pemilik yang mengirimkan informasi tersebut.

METODE PENELITIAN

Metode yang digunakan untuk memperoleh data adalah metode studi literatur, yaitu dengan membaca sejumlah buku, artikel dan sumber lain untuk memperoleh data teoritis serta pemahaman mengenai permasalahan yang akan dibahas dalam penelitian ini.

HASIL PENELITIAN

Pada bab ini akan dilakukan pembahasan berdasarkan data dan fakta yang sudah dijabarkan sebelumnya dengan berlandaskan teori yang ada di subbab sebelumnya. Untuk pembahasan, akan dijelaskan berikut ini.

Skenario Proteksi Yang Diberikan IRM

Terdapat beberapa cara yang sudah lebih familier untuk digunakan dalam mengatasi kebocoran informasi yang biasanya membatasi akses kepada jalur-jalur data dan informasi dalam jaringan komunikasi organisasi, namun biasanya tidak memberikan proteksi yang terkait dengan informasi itu sendiri.

Proteksi menggunakan IRM dapat dilakukan pada dua aspek, yang pertama adalah melakukan proteksi pada dokumen informasi yang dikirimkan sebagai lampiran/*attachment* yaitu dengan mengaktifkan IRM pada dokumen-dokumen MS. Office yang berisi informasi rahasia/terbatas, sedangkan yang berikutnya adalah pada aspek email itu sendiri dengan mengaktifkan IRM pada Microsoft Outlook (Turick, 2003).

Dalam skala kecil IRM dapat juga digunakan oleh individu untuk melakukan proteksi terhadap informasi-informasi pribadi yang tidak ingin tersebar luas ketika dilakukan pengiriman informasi tersebut, sedangkan dalam skala yang lebih luas IRM dapat membantu sebuah organisasi untuk mengelola dan menerapkan kebijakan yang terkait dengan perlindungan aset/properti intelektual organisasi, sehingga dalam proses distribusi informasi tersebut kepada pihak-pihak yang

berkepentingan tetap memiliki kontrol yang melindungi kepemilikan dari informasi tersebut. Jadi tidak masalah apakah digunakan dalam skala kecil oleh individu ataupun digunakan dalam skala yang lebih besar oleh sebuah organisasi, IRM dapat memberikan dampak yang signifikan terhadap risiko jatuhnya informasi kepada pihak-pihak yang dapat menyalahgunakan informasi tersebut atau dapat merugikan pemilik informasi.

Menurut Microsoft Corporation (2011) ada beberapa hal yang dapat dilakukan oleh IRM dalam upaya memberi proteksi terhadap distribusi informasi, yaitu:

i. Membantu mencegah penerima informasi yang tidak memiliki wewenang untuk melakukan penerusan, penggandaan, modifikasi, pencetakan, dan mencuplik informasi yang didistribusikan.
ii. Mencegah terjadinya penyalahgunaan /pencurian informasi dengan cara digandakan menggunakan fungsi print-screen yang ada pada Windows
iii. Memberikan proteksi pada level yang sama ke manapun informasi tersebut terdistribusi atau disebut "*persistence protection*".
iv. Memberikan proteksi yang konstan untuk informasi yang dikirim melalui lampiran/*attachment* email selama informasi tersebut dibuat dalam format yang ada pada program MS. Office seperti Word dan Excel.
v. Membantu melindungi informasi pada email atau dokumen yang dilampirkan dengan menerapkan batas waktu kadaluwarsa, sehingga informasi yang didistribusikan tidak lagi dapat dibaca setelah periode waktu tertentu.
vi. Membantu penerapan kebijakan organisasi dalam mengelola penggunaan dan pendistribusian informasi di dalam dan di luar organisasi.

Selain hal-hal yang dapat dilakukan dengan menggunakan IRM sebagaimana tersebut di atas, terdapat juga beberapa hal yang tidak dapat dilakukan oleh IRM dalam usaha proteksi informasi sehingga perlu dilakukan antisipasi lanjutan [6]. Hal-hal yang tidak dapat dilakukan tersebut di antaranya sebagaimana tersebut di bawah ini:

i. Melindungi informasi yang dikirimkan kepada penerima pesan untuk tidak terhapus, dicuri, dibajak dan ditransmisikan oleh program-program yang bersifat merusak seperti *trojan horses, keystroke loggers,* dan beberapa jenis *spyware*.

ii. Mencegah hilangnya sebagian atau keseluruhan dari informasi akibat dari operasi virus pada komputer.

iii. Mencegah informasi untuk tidak digandakan dengan cara ditulis ulang oleh penerima pesan atau mengambil gambar yang terdapat pada tampilan monitor penerima pesan.

iv. Mencegah penggandaan informasi dengan menggunakan *third-party screen-capture programs*.

Dokumen Informasi Yang Dapat Diproteksi Menggunakan IRM

Menurut Microsoft Corporation (2011) proteksi dengan menggunakan IRM dapat dilakukan terhadap beberapa jenis *file*/dokumen yang dibuat dengan menggunakan program dari MS. Office. Berikut ini beberapa jenis *file*/dokumen yang dapat diproteksi menggunakan IRM sehingga dalam proses distribusinya dapat memiliki kontrol yang tetap pada level yang sama ke manapun informasi tersebut didistribusikan:

i. *File*/dokumen yang dibuat dengan menggunakan MS. Word.

File type	Extension
Document	.doc
Document	.docx
Macro-enabled document	.docm
Template	.dot
Template	.dotx
Macro-enabled template	.dotm

ii. *File*/dokumen yang dibuat dengan menggunakan MS. Excel.

File type	Extension
Workbook	.xls
Workbook	.xlsx
Macro-enabled workbook	.xlsm
Template	.xlt
Template	.xltx
Macro-enabled template	.xltm
Non-XML binary Workbook	.xlsb
Macro-enabled add-in	.xla
Macro-enabled add-in	.xlam

iii. *File*/dokumen yang dibuat dengan menggunakan MS. PowerPoint.

File type	Extension
Presentation	.ppt
Presentation	.pptx
Macro-enabled Presentation	.pptm
Template	.pot
Template	.potx
Macro-enabled template	.potm
Show	.pps
Show	.ppsx
Macro-enabled show	.ppsm
Office theme	.thmx

Jika seseorang melakukan proteksi terhadap dokumen Ms. Office, maka dokumen tersebut akan dienkripsi dan isinya akan dikodekan dalam bentuk yang tidak bisa dipahami jika dilihat apa adanya (Zhou, 2006). Selain itu program yang

akan digunakan untuk membuka dokumen tersebut juga harus terlebih dahulu mengaktifkan *feature* IRM.

Perlu dicatat bahwa jika jenis *file*/dokumen tersebut di atas dilampirkan dalam e-mail yang menerapkan IRM seperti dalam pesan Microsoft Outlook misalnya, maka *file*/dokumen tersebut akan secara otomatis menerapkan juga IRM. Namun jika yang dilampirkan dalam email adalah sebuah pesan dengan ekstensi (.msg), maka terhadap informasi yang dilampirkan tersebut tidak akan diterapkan IRM meskipun dilampirkan dalam email yang sudah menerapkan fungsi IRM, karena IRM tidak dapat mengelola jenis *file*/dokumen dengan ekstensi seperti (.msg) tersebut (Microsoft Corporation, 2011).

Mengaktifkan Feature IRM

Sebagaimana telah disinggung sebelumnya bahwa IRM memberikan teknologi proteksi yang berjalan pada level yang sama pada setiap komputer dengan menggunakan program-program dari MS. Office. Dokumen dalam bentuk Word, Excel dan yang lainnya sering kali didistribusikan dalam bentuk lampiran email atau mungkin juga di-*share* dalam *server* dokumen organisasi misalnya dengan menggunakan Microsoft Windows Server 2003 yang memiliki Windows Rights Management Services.

Meskipun IRM adalah layanan *free service*, namun untuk mengaktifkan IRM pertama kali dibutuhkan sebuah Microsoft.NET *passport* yang juga dapat diperoleh secara gratis. Selain itu perlu dilakukan instalasi terhadap IRM *client software* di komputer yang akan digunakan untuk membuat proteksi terhadap dokumen tersebut.

Berikut akan disajikan langkah-langkah bagaimana mengaktifkan IRM dalam organisasi dan dalam hal ini diambil contoh dari MTR-IRM *User Guide* (2011).

i. Pimpinan organisasi atau pejabat yang berwenang menetapkan kebijakan terkait dengan distribusi dokumen yang bersifat rahasia berupa siapa yang dapat menerima dan membaca dokumen tersebut serta kapan dokumen tersebut dapat dibaca.

ii. Memilih menu File->Prepare->Restrict Permission->Restricted Acces dalam program Ms. Office yang digunakan untuk membuat dokumen.
iii. Setelah itu akan muncul *dialogue box* yang dapat menampilkan *user account* berupa alamat email yang dapat diatur *user account* apa yang akan digunakan untuk melakukan pengaturan terhadap kebijakan distribusi dokumen tersebut.

Menetapkan Batasan Terhadap Informasi Yang Akan Didistribusikan

Ketika IRM telah diaktifkan, maka setiap dokumen yang berisi informasi terbatas dapat diproteksi dengan menggunakan IRM setelah terlebih dahulu ditetapkan batasan distribusi informasi tersebut.

Batasan-batasan yang ditetapkan dapat berupa *user account* yang dapat membaca pesan dalam dokumen yang didistribusikan serta kapan dokumen tersebut kadaluwarsa. Berikut beberapa langkah yang dapat dilakukan dalam menetapkan batasan terhadap informasi yang didistribusikan:

i. Setelah mengisi *dialogue box* sebagai mana pada poin 4.3 butir (iii) pada bagian Mengaktifkan *Feature* IRM, maka akan muncul *Permission dialogue box* yang dapat kita isi dengan *list user account*nyang akan kita set sebagai tujuan/penerima informasi yang kita distribusikan
ii. Pada *dialogue box* tersebut dapat kita isi nama-nama pada kolom yang disediakan, apakah penerima dokumen hanya dapat membaca dokumen atau juga dapat melakukan modifikasi atau perubahan pada dokumen yang didistribusikan.
iii. Jika diperlukan untuk melakukan pengaturan otorisasi yang lebih detail terhadap *user account* yang telah dipilih, dapat dilakukan pengaturan dengan memilih *More Option* pada *dialogue box*.

Access level atau *Permission Level* yang diberikan dapat diubah dengan memilih beberapa tingkat seperti di bawah ini: [6]

a. ***Read*** level yang memberikan *read permission* kepada *user* yang dipilih untuk dapat membaca dokumen namun tidak dapat melakukan modifikasi, pencetakan, maupun mengopi dokumen tersebut.
b. ***Change*** level yang memberikan *change permission* kepada *user* yang dipilih dan ini berarti *user* tersebut dapat membaca dokumen, melakukan modifikasi terhadap

dokumen dan menyimpan perubahan tersebut namun tidak diberikan kewenangan untuk melakukan pencetakan dokumen.

c. ***Full Control*** level yang memberikan *full control permission* kepada *user* yang dipilih sehingga *user* tersebut memiliki wewenang untuk melakukan tindakan-tindakan sebagaimana yang dimiliki oleh pembuat dokumen seperti melakukan pengaturan tanggal kadaluwarsa, pengaturan kepada *user* lain, pengaturan pencetakan dokumen, dan lainnya. Setelah lewatnya tanggal kadaluwarsa yang ditetapkan atas dokumen, hanya pembuat dokumen dan *user* dengan *access* level *Full Control* yang dapat membuka dokumen tersebut, hal ini dikarenakan seorang pembuat dokumen akan selalu memiliki *access* level *Full Control* atas dokumen yang dibuatnya.

Menggunakan IRM Pada Email

IRM dapat langsung diaplikasikan pada email dengan menggunakan MS. Outlook. Dengan mengaktifkan *permission setting* menjadi "*Do Not Forward*", maka email yang terkirim akan terproteksi dan menjadi bersifat terbatas pada *user account* yang ditentukan oleh pengirim dan tidak dapat diteruskan kepada *user account* lain, dan juga tidak dapat di *copy-paste* ke tempat lain.

Jika dalam email yang mengaktifkan IRM terdapat lampiran berupa dokumen MS. Office, maka secara otomatis dokumen tersebut juga akan diproteksi oleh IRM sehingga memiliki sifat terbatas seperti email yang dikirimkan.

Menggunakan IRM Pada Lampiran Email

Dokumen yang berisi informasi terbatas sering kali dilampirkan dalam sebuah email untuk didistribusikan. Jika email yang digunakan tidak mengaktifkan IRM, maka dokumen MS. Office yang dilampirkan pada email tersebut dapat kita proteksi sehingga memiliki proteksi yang melindungi dari tindakan-tindakan yang tidak dikehendaki oleh pengirim dokumen.

Jika yang kita proteksi hanya lampiran dalam email, maka email tersebut masih dapat diteruskan kepada *user account* lain, namun untuk membaca dokumen yang

dilampirkan harus mengajukan permintaan izin kepada *user account* pembuat dokumen untuk diberikan akses terhadap dokumen tersebut.

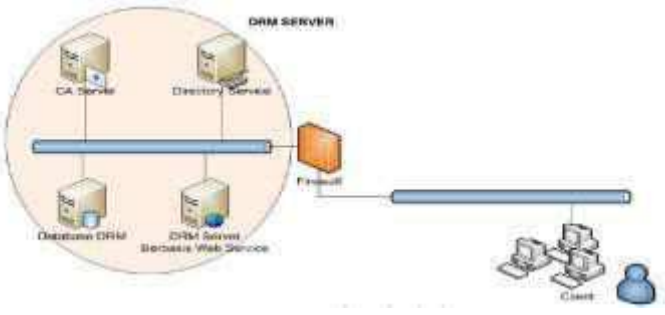
Prinsip Kerja IRM

Setiap dokumen elektronik yang telah dibuat dan ingin memproteksi informasi didalamnya maka terhadap dokumen elektronik tersebut dapat diterapkan *Digital Rights Management* (DRM). Proses ini melibatkan enkripsi berbasis kriptografi yang mempunyai *public key* dan *private key*. Sistem yang menghasilkan *public key* dan *private key* dapat berperan sebagai *license server*.

Secara umum implementasi aplikasi yang menerapkan DRM dapat menggunakan pendekatan arsitektur *client-server*. *Server* disini menyediakan layanan:

i. Menghasilkan *public key* dan *private key* terhadap setiap dokumen elektronik yang akan menerapkan DRM.
ii. Menghasilkan *license* yang berisi informasi hak apa saja dapat ditujukan pada dokumen tersebut.
iii. Menyimpan semua data DRM dari setiap dokumen. Hal ini dilakukan pada bagian *database server*.

Semua komponen yang terlibat dimasukkan ke dalam domain direktori yang sama sehingga sistem authentikasi dan otorisasi dapat dikontrol secara terpusat.



Gambar Desain lokal pada sistem DRM

IRM dari Microsoft menggunakan suatu prinsip kerja seperti DRM yang lain. Prinsip kerja dokumen elektronik yang akan menerapkan DRM diawali dengan beberapa langkah yang dilakukan oleh *user account* pemilik dokumen dengan proses sebagai berikut ini:

1. User pemilik dokumen yang bermaksud untuk memproteksi dokumen harus mendaftarkan komputer dan domain *user account* ke DRM *Certificate Authority* (CA). Mesin komputer yang sudah didaftarkan akan mendapatkan *machine certificate* sedangkan identitas *user account* akan memperoleh *Rights Account Certificate* (RAC).
2. Selanjutnya *user* akan melakukan *download certificate* dari DRM *Server* dan mengaktifkannya.
3. Setelah *user* mengaktifkan *certificate*, user membuat *issuance license* yang berisi hak akses yang akan diterapkan pada dokumen tersebut seperti *Read-Only, Don't Forward, Editable, Print* dan sebagainya. *Issuance license* juga dapat diberlakukan masa aktifnya sesuai dengan kebutuhan.
4. *Issuance license* yang telah dibuat kemudian dikirim ke DRM *Server* untuk dilakukan proses *signing* sehingga nantinya dapat didistribusikan apabila user lain mengakses dokumen ini. *User* pemilik *issueance license* akan memperoleh *owner license*.
5. Dengan menggunakan *owner license*, *user* kemudian melakukan proses *editing* dokumen
6. Apabila proses *editing* telah selesai dilakukan, maka aplikasi akan melakukan enkripsi isi dokumen dan mengirimnya ke DRM *Server.*

Sedangkan bagi *user* lain yang ingin mengakses dokumen berbasis DRM maka proses yang dilakukan adalah: [10]

1. Ketika *user* membuka dokumen berbasis DRM maka aplikasi *client* yang mengenali DRM akan meminta *end-user license* ke DRM *Server* dengan dengan informasi yang ada pada dokumen DRM tersebut.

2. Sebelum memperoleh *end-user license* maka *user* akan dicek melalui *directory service* apakah *user* tersebut merupakan anggota dari DRM *Server* atau tidak.

3. Apabila proses pengecekan selesai dan ternyata bukan anggota DRM maka *user* tersebut tidak dapat memperoleh *end-user license.*

4. Jika *user* merupakan anggota DRM maka *user* akan memperoleh *end-user license* dari DRM *Server.*

5. *End-user license* berisi informasi hak akses yang dimiliki terhadap dokumen yang dibuka.

6. Apabila *user* mempunyai hak akses (minimal dapat melihat/*Read-Only*) maka aplikasi akan melakukan dekripsi melalui *public key* yang sudah disediakan.

Apabila dokumen DRM ini diletakan pada email sebagai lampiran, maka pada dasarnya aplikasi *client* email akan melampirkan suatu dokumen yang terenkripsi. Kemudian *user* mengirim email dengan lampiran dokumen DRM ke tujuan. Setelah sampai pada target penerima maka lampiran

Mengaplikasikan IRM Pada Organisasi Publik

Organisasi terutama dalam pemerintahan sangat identik dengan dokumen rahasia dan bersifat terbatas, namun demikian upaya pencegahan penyalahgunaan atas dokumen rahasia tersebut sepertinya belum optimal.

Berdasarkan pada pengamatan di beberapa instansi pemerintah, secara umum pengamanan arus informasi dalam jaringan teknologi informasi yang selama ini digunakan biasanya lebih berorientasi pada keamanan jaringan organisasi. Hal ini dapat dilihat dengan diberlakukannya *security log-on* dan penggunaan *firewall* pada jaringan dan perangkat komputer di instansi-instansi pemerintah. Hal ini sangat membantu dalam membatasi pencurian informasi oleh pihak luar seperti serangan "*man in the middle attack*", namun tidak mampu mengontrol dokumen begitu

dokumen tersebut diunduh ke dalam *hard disk* lokal, sehingga bisa dengan mudah dipindah tangankan melalui USB *flash drive* atau cara-cara lain.

Secara infrastruktur tidak diperlukan investasi besar untuk menerapkan IRM sebagai salah satu upaya mengamankan informasi pada organisasi pemerintah. Namun demikian, perlu dipersiapkan beberapa hal sebelum organisasi pemerintah dapat menerapkan IRM dengan baik sebagai bagian dari kebijakan organisasi yaitu:

i. Memiliki *Data Governance and Classification Policy.* Untuk dapat menetapkan informasi yang terdapat dalam organisasi diperlukan pengelolaan dan kebijakan yang memberikan definisi dari informasi-informasi yang ada, apakah ada informasi yang bersifat rahasia/terbatas dan seperti apa pengelolaan yang ditetapkan atas informasi tersebut.
ii. Menetapkan informasi mana saja yang bersifat rahasia dan berada pada wewenang siapakah informasi tersebut, serta siapa saja yang memerlukan penggunaan informasi tersebut.
iii. Menetapkan bagaimana otorisasi akan diberikan kepada setiap pegawai yang ada dalam organisasi, apakah akan menggunakan satu sistem otorisasi dan berlaku untuk semua jenis informasi, atau akan diterapkan otorisasi yang dinamis.
iv. Menetapkan standar yang jelas terkait keadaan yang diharapkan setelah menetapkan IRM sebagai bagian dari pengelolaan informasi organisasi.
v. Diperlukan pengawasan apakah penerapan teknologi IRM berpengaruh positif terhadap proses bisnis organisasi atau justru memberi dampak negatif.
vi. Menyusun mekanisme audit atas kepatuhan terhadap kebijakan organisasi dalam menetapkan batasan-batasan terhadap organisasi.

KESIMPULAN

Dengan uraian tersebut di atas, dapat dimengerti bahwa keamanan atas informasi tidak hanya terbatas pada keamanan jaringan sebagai tempat lalu lintas informasi tersebut. Salah satu faktor yang harus diperhatikan adalah bagaimana distribusi atas dokumen yang berisi informasi rahasia/terbatas.

IRM merupakan salah satu solusi cepat yang dapat diimplementasikan untuk mengatasi masalah penyalahgunaan informasi. Hal ini berlaku dalam skala kecil seperti individu maupun dalam skala yang besar seperti sebuah organisasi.

Kelebihan yang ada pada IRM yaitu menyediakan keamanan dari sisi dokumen informasi dapat dioptimalkan bersama dengan keamanan secara jaringan dan penyimpanan data dalam *database*. Dengan demikian, setiap informasi yang bersifat terbatas/rahasia dapat terjaga dan terkontrol baik ketika terdistribusi maupun ketikan tersimpan dalam *hard disk* lokal organisasi. Keamanan yang bersifat menyeluruh ini diharapkan dapat memenuhi keseluruhan aspek dari keamanan informasi yaitu *confidentiality, integrity,* dan *availability*.

Pemanfaatan IRM organisasi publik dapat memberikan perlindungan tambahan yang memadai terhadap distribusi informasi-informasi penting yang bersifat rahasia. Hal ini dikarenakan kewenangan yang ada pada masing-masing pegawai dibatasi sesuai dengan otorisasi yang diberikan oleh pemilik informasi.

DAFTAR PUSTAKA (*REFERENCES*)

Danny Lieberman. *Preventing Intellectual Property Abuse, A Comparison Between Information Rights Management and Data Loss Prevention.* Creative Commons Attribution License. 2009

Hong Zhou. *Evaluation of Certificate Revocation in Microsoft Information Rights Management v1.0.* October 2006

Information *Rights Management Solution: Securing Information Exchange in Outsourcing Arrangements*, Infosys Limited, 2010

IRM User Guide, MTR, 2011

John Prathab, 2011. *Important Question to Ask Before Deploying Information Rights Management.* (Seclore)
Available at: http://blog.seclore.com

Kurniawan, A. (2010), Digital Rights Management Sebagai Solusi Keamanan Dokumen Elektronik, *Jurnal Sistem Informasi MTI UI,* 4 (2), 93 -99.

Microsoft Corporation, 2011. *Information Rights Management in the 2007 Microsoft Office system.* (Microsoft Office) [online]
Available at: http://office.microsoft.com

Queensland Government (2008), "*What is Microsoft Information Rights Management?*. Queensland: Queensland State Archive.

Romney, Steinbart. (2015). *Accounting Information System, 13th ed.* Pearson Education, Inc. New Jersey.

Turick J. (2003). *Information Rights Management in Microsoft Office Outlook 2003©* Microsoft Corporation.

Viktor Mayer-Schönberger. Beyond Copyright: Managing Information Rights With DRM. *Denver University Law Review,* 84 (1), 181 – 198.

Yang Yu and Tzi-cker Chiueh. *Enterprise Digital Rights Management: Solutions against Information Theft by Insiders.* Computer Science Departement. Stony Brook University.